IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Graeme John Proudler	) On Appeal to the) Board of Appeals
Patent Application No.: 10/643,306	)
Filed: 08/18/2003	) Group Art Unit: 2135)
For: "A method of controlling the processing of data"	) Examiner: Dada, B.W.)) Date: March 18, 2008)

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the Final Rejection (or Final Action), dated October 19, 2007, for the above identified patent application. Appellants submit that this Appeal Brief is being timely filed on March 18, 2008, because the Notice of Appeal was filed on January 18, 2008. Please charge the Appeal Brief fee of $510.00 to deposit account no. 08-2025.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC

RELATED APPEALS AND INTERFERENCES

Appellants submit that there are no other prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-43 and 50 are present in the application, are the subject of this Appeal and are reproduced in the accompanying Claims appendix.

STATUS OF AMENDMENTS

A claim amendment canceling claims 44 and 46-49 has been filed under 37 CFR 1.116 in response to the Final Rejection in order to narrow the issues which must be considered in this appeal. The applicant has not yet been advised by the Examiner that this amendment has been entered, but the Examiner advises that this amendment should be entered by the same week that this appeal brief is filed.

SUMMARY OF CLAIMED SUBJECT MATTER

The version of this application as published by the USPTO is not correct so the Board should not rely on that version of the present application. A request for republication has been filed.

The present application concerns itself with the protection of private data (see Fig. 1 and p. 11, ll. 19-32) in the context of trusted computing platforms (TCP; Fig. 5) of the type which provide a measurement of the integrity (p. 18, ll.4-12) of the TCP, that is, a measurement of whether the TCP can really be trusted with private data.

Claim 1 is directed to a method of controlling processing of data in a computer apparatus (TCP; Fig. 5), wherein the data comprises a plurality of usage rules (50) for a plurality of data items (52; 54; 56 ... 60; see Figs. 1 and 3, and p. 11, l. 19 through p. 13, l. 26) stored by said computer apparatus, and comprising:

applying individualised usage rules to each of the data items (Fig. 3, p. 13, ll. 12-20) based on a measurement of integrity of a computing entity to which the data items are to be made available (see rule 'M' in Fig 3, for example and see p. 17, l. 1 through p. 18, l. 12), said data items being logically grouped together as a set of data items (Fig. 3 and p. 14, ll. 1-16), and

instantiating the set of data items at the computing entity depending upon the integrity (p. 17, l. 1 through p. 18, l. 12) of the computing entity and the usage rule applicable to each data item in said set (see p 15, l. 27 through p. 19, l. 2 and p. 20, ll. 9-12).

Claim 33 is directed to a method of controlling processing of data, wherein the data comprises a plurality of rules (50) associated with a plurality of data items (52; 54; 56 ... 60; see Figs. 1 and 3, and p. 11, l. 19 through p. 13, l. 26) comprising a set of

logically related data items (Fig. 3 and p. 14, ll. 1-16), each data item in the set having a rule associated therewith (Fig. 1), said rules acting to individually define usage and/or security to be observed when processing each of the data items in the set of data items (see Fig. 3), and in which forwarding of the set of data items is performed in accordance with mask means (see p. 18, ll. 27-29) provided in association with the rules.

Claim 43 is directed to a computer program stored on computer readable media for instructing a programmable computer to implement a method of controlling the processing of data, wherein the data comprises a plurality of usage rules (50) for a plurality of data items (52; 54; 56 ... 60; see Figs. 1 and 3, and p. 11, l. 19 through p. 13, l. 26), the programmable computer being programmed to apply individualised usage rules to each of the data items (see Fig. 3) based on a measurement of integrity of a computing entity (p. 17, l. 1 through p. 18, l. 12) to which the data items are to be made available, the computer program permitting instantiation of the data items at the computing entity only if the integrity of the computing entity complies with the individualised usage rules associated with said data items (see p 15, l. 27 through p. 19, l. 2 and p. 20, ll. 9-12).

Claim 50 is directed to a computer apparatus for controlling processing of data, wherein the data comprises a plurality of usage rules for a plurality of data items stored by said computer apparatus, said computer apparatus controlling instantiation of the data at a computing entity, said computer apparatus including:

programming for applying individualised usage rules (50) to each of the data items (52; 54; 56 ... 60; see Figs. 1 and 3, and p. 11, l. 19 through p. 13, l. 26) based on a measurement of integrity of the computing entity to which the data items are to be made available, said data items being logically grouped together as a set of data items (Fig. 3 and p. 14, ll. 1-16), and

programming for individually instantiating data items in the set of data items at the computing entity as a function of the integrity of the computing entity and

the usage rule applicable to each data item in said set (see p 15, l. 27 through p. 19, l. 2 and p. 20, ll. 9-12).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether Claims 1-43 and 50 are patentable under 35 U.S.C. 103(a) in view of Raley, US patent publication US 2003/0196119 (hereinafter " Raley") in view of Ishizaki, US patent publication US 2002/0019934 (hereinafter " Ishizaki")?

ARGUMENT

Issue 1: Whether Claims 1-43 and 50 are patentable under 35 U.S.C. 103(a) in view of Raley, US patent publication US 2003/0196119 (hereinafter " Raley") in view of Ishizaki, US patent publication US 2002/0019934 (hereinafter " Ishizaki")?

In the final Office Action of October 19, 2007, the Examiner rejects Claims 1-43 and 501 under 35 U.S.C. 103(a) as being obvious to one of ordinary skill based on Raley and Ishizaki. Appellant respectfully disagrees.

---

[1] In paragraph 7 the Examiner mentions claim 49, but in paragraph 8 the Examine mentions 50. It is believed that the rejection was intended to be directed towards claim 50.

The Raley Reference

Raley's disclosure relates to distribution of digital content (web pages), and more particularly, to a method and apparatus for facilitating distribution of protected documents (web pages) displayed using the rendering engine of a standard application program, such as an Internet Web Browser, at a user's computer. The user's browser must have an end user interface (UI) module (234) installed or the website delivering the digital content will refuse to deliver the content to the end user.

The Ishizaki Reference

Ishizaki's disclosure is concerned with providing encryption and decryption apparatuses, methods, and computer program products capable of selectively encrypting and decrypting a part of file portions being handled on a computer, particularly, selectively encrypting and decrypting data portions in specified association with an item name of a database, thereby making it possible to protect against unauthorized use and tampering while major database features are enabled.

Is it obvious to combine the teachings of Raley and Ishizaki?

The examiner points to Raley's documents 222 (web pages) and reads them on the limitation "data items" recited in the claims. Independent claims 1,33 and 50 each recite that the data items are "logically grouped together as a set of data items" or "a set of logically related data items". The Examiner admits that Raley does not teach this latter feature, but points to Ishizaki and makes the conclusory statement that "it would have been obvious ... to logically group a set of data items ... and employ it within the data of Raley to achieve the predictable result of grouped based controlling of processing of data" [see item 8 in the Official Action]. The Applicant's response is that the Examiner is playing fast and loose here. Raley documents 222 (web pages) somehow

morph into "data items" such as one might see in a normal database in this analysis. The data within a single row of a normal database is usually grouped, but the row items are not grouped. In Raley individual documents are more akin to row items of a database, so why group them? And exactly what "predictable result" in terms of improving upon Raley would occur of these documents are somehow grouped?

Of course, 35 U.S.C. § 103 "forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1734 (2007). The Court stated that obvious analysis "should be made explicit." Id. at 1740-41, citing *In re Kahn*, 441 F.3d 977,988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness").

The Examiner asserts in the Final Official Action that a person of ordinary skill would be motivated to modify the teachings of Raley by the teachings of Ishizaki "to logically group a set of data items ... and employ it within the data of Raley to achieve the predictable result of grouped based controlling of processing of data". If the grouping of data of Ishizaki is "employed within the data of Raley", as asserted by the Examiner, then that suggests that a single Raley webpage is supposed to get the Ishizaki treatment. If that is the case, then it is the words within a single Raley document (webpage) which get grouped and not the documents (webpages) which are somehow arranged in groups. But the claim language of these claims recite that the data items are "logically grouped together as a set of data items" or "a set of logically related data items". Grouping the words in a single Raley document (webpage) in accordance with Ishizaki does not meet this language. One does not arrive at a set of webpages by folloeing the Examiner's analysis!

The examiner's statements are not only difficult to follow, but are merely conclusory statement. The Examiner has provided no articulated reasoning with some rational underpinning to support his legal conclusion of obviousness. The rejection under 35 USC 103(a) is improper and should be overturned.

If it is obvious to combine the teachings of Raley and Ishizaki, then do they teach each and every limitation of the claims?

Appellants submit that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP 2131 quoting *Verdegaal Bros. V. Union Oil Co, of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The Examiner is also reminded that "[the] identical invention must be shown in as complete detail as is contained in the ... claim." MPEP 2131 quoting *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Appellants submit that the Examiner has not shown that Raley even when combined with Ishizaki teaches each and every element as set forth in the rejected claims. In particular:

Independent Claims 1, 43 and 50

Claims 1, 43 and 50 each include a limitation along the following lines: "applying individualised usage rules to each of the data items based on a measurement of integrity of a computing entity to which the data items are to be made available". Support for the various forms of this limitation can be found at Figure 3 where certain data items, "County" and "City" have a rule "M" associated with them restricting them from being sent to non-trusted platforms. Note that the entries at the middle of Fig. 3 would be typical columnar headings in a typical database.

The Examiner tried to read this limitation on Raley's documents 222 and their associated usage rights and the test which is made to see if the client has a required browser right management module (234) installed [noting paragraph 0052 of Raley].

Raley's test to see if a browser has a UI module 324 installed is not a test of the "measurement of integrity of a computing entity" as claimed (Raley checks the browser, not the computing entity) and even if it were a test of the computing entity, the test is not "individualized" as claimed. In applicant's specification, the different data items can be treated differently according to the tests performed. So individualization based upon the integrity of a computing entity to which the data items are to be made available is apparent. In Raley apparently all documents are treated equal in this regard ... there is no "applying individualised usage rules to each of the data items based on a measurement of integrity of a computing entity to which the data items are to be made available" as recited by claim 1 and 50 or the "to apply individualised usage rules to each of the data items based on a measurement of integrity of a computing entity to which the data items are to be made available" recited by claim 43. Raley does not meet all of the limitations of these claims and the Examiner has pointed to nothing outside of Raley as meeting these limitations!

Independent Claim 33

Independent claim 33 recites "a set of logically related data items, each data item in the set having a rule associated therewith, said rules acting to individually define usage and/or security to be observed when processing each of the data items in the set of data items, and in which forwarding of the set of data items is performed in accordance with mask means provided in association with the rules." The Examiner reads this limitation on basically the same disclosure of Raley outlined above, but also relies on Raley's encryption/decryption discussed in paragraph 0053 of Raley.

In Raley it appears that all documents 222 are treated equal when it comes to their treatment if the user does not have module 234 installed in their browser. Raley does not "individually define usage and/or security to be observed when processing each of the data items in the set of data items" as claimed.

Moreover, how is a "set of data items" supposed to be defined based on Raley? Since the Examiner reads the limitation "data item" on Raley's documents/webpages, how is a "set" ever formed? Where does "processing each of the data items in the set of data items" occur in Raley?

Turning to the limitation "in which forwarding of the set of data items is performed in accordance with mask means", that is supported by the disclosure at the paragraph which bridges pages 18 and 19 of the application as filed. Here set of data item(s) is/are masked from the recipient of the other data being sent so that the identity of the user is protected. Raley's encryption/decryption discussed at paragraph 0053 does not mask the recipient from any set of data items. It is unreasonable to read Raley's encryption/decryption on the claimed "forwarding of the set of data items is performed in accordance with mask means" in view of applicant's disclosure.

Conclusion

For the extensive reasons advanced above, Appellants respectfully contend that each claim is patentable. Therefore, reversal of all rejections and objections is courteously solicited.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this Appeal Brief is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this paper (and any enclosure referred to in this paper) is being transmitted electronically to the United States Patent and Trademark Office on

March 18, 2008
(Date of Transmission)

Stacey Dawson
(Name of Person Transmitting)

/Stacey Dawson/
(Signature)

March 18, 2008
(Date)

Respectfully submitted,

/Richard P. Berg/

Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile

Encls:
Claims Appendix;
Evidence Appendix;
Related Proceedings Appendix.

1. A method of controlling processing of data in a computer apparatus, wherein the data comprises a plurality of usage rules for a plurality of data items stored by said computer apparatus, and comprising:

applying individualised usage rules to each of the data items based on a measurement of integrity of a computing entity to which the data items are to be made available, said data items being logically grouped together as a set of data items, and

instantiating the set of data items at the computing entity depending upon the integrity of the computing entity and the usage rule applicable to each data item in said set.

2. A method as claimed in claim 1, in which at least some of the usage rules comprise masking instructions for masking the associated data items.

3. A method as claimed in claim 2, in which a data item is masked from a set of data by encrypting it.

4. A method as claimed in claim 3, in which a data item is encrypted with an associated encryption key, said encryption key being different for different ones of the data items.

5. A method as claimed in claim 1, in which the usage rules define security rules for the associated data item.

6. A method as claimed in claim 1, in which the data may be transferred between a plurality of computing entities and the instantiation of the data at each computing entity depends on the capabilities of that entity.

7. A method as claimed in claim 6, in which a computing entity is a computing platform.

8. A method as claimed in claim 6, in which the computing entity is a software process.

9. A method as claimed in claim 1, in which a computing entity can reliably and irrevocably deny future access to selected data items.

10. A method as claimed in claim 9, in which means for accessing the data is stored within a protected memory.

11. A method as claimed in claim 10, in which the protected memory is within a trusted computing module.

12. A method as claimed in claim 1, in which computing entities negotiate with one another concerning the use of the data before the data is made available.

13. A method as claimed claim 1, in which the data has constraints defining conditions for use of the data.

14. A method as claimed in claim 13, in which the constraints define at least one item selected from:

a. the purpose for which the data can be used

b. the geographical area in which the data may be manifested

c. the temporal domain in which the data may be manifested

d. the computing platforms that may manipulate the data.

15. A method as claimed in claim 1 in which the data further includes test data.

16. A method as claimed in claim 15, in which the structure of test data is comparable to the structure of real data contained by the data items.

17. A method as claimed in claim 16, in which the results of operations performed on the test data are examined in order to make a decision on whether to release the real data to a node that operated on the test data.

18. A method as claimed in claim 1, in which a node requesting access to the data supplies hostage material to the node issuing the data prior to the issuance of the data.

19. A method as claimed in claim 18, in which a third party hostage release authority is contacted to activate the hostage material.

20. A method as claimed in claim 1 in which a node finding itself in possession of data whose history or content do not meet predetermined requirements, formats the data and places it in a repository.

21. A method as claimed in claim 20, in which the data placed in the repository is in an encrypted form.

22. A method as claimed in claim 21, in which the data is encrypted using a public key included in the data.

23. A method as claimed in claim 21, in which the data in the repository is associated with an identification means to enable the owner of the data to identify it.

24. A method as claimed in claim 1, in which a node wishing to present the data for retrieval places the data in a repository.

25. A method as claimed in claim 24, in which the data is placed in the repository in encrypted form.

26. A method as claimed in claim 25, in which the data is encrypted using a public key included in the data.

27. A method as claimed in claim 26, in which the data in the repository is associated with identification means to enable the owner of the data to identify it.

28. A method as claimed in claim 1, in which constraints associated with the data determine whether the data will process on anything other than a trusted computing platform.

29. A method as claimed in claim 28, in which constraints associated with the data determine whether the data and/or results from processing the data are inhibited from viewing by a computing platform owner or administrator.

30. A method as claimed in claim 1 in which the security contracts are stored separately from the data.

31. A method as claimed in claim 1 in which mask or decryption keys are stored separately from the data.

32. A method as claimed in claim 1 in which a computing entity that receives data signs the data with a signature key belonging to that entity.

33. A method of controlling processing of data, wherein the data comprises a plurality of rules associated with a plurality of data items comprising a set of logically related data items, each data item in the set having a rule associated therewith, said rules acting to individually define usage and/or security to be observed when processing each of the data items in the set of data items, and in which forwarding of the set of data items is performed in accordance with mask means provided in association with the rules.

34. A method as claimed in claim 33, in which the mask comprises at least one of a symmetric encryption string, symmetric encryption key, and an asymmetric encryption key.

35. A method as claimed in claim 33, in which the rules associated with the data items are adhered to in preference to data handling rules associated with a computing entity processing the data.

36. A method as claimed in claim 33, in which at least some of the rules comprise masking instructions for masking the associated data items.

37. A method as claimed in claim 36, in which a data item is masked from a set of data by encrypting it.

38. A method as claimed in claim 37, in which a data item is encrypted with an associated encryption key, said encryption key being different for different ones of the data items.

39. A method as claimed in claim 33 in which the data may be transferred between computing entities and the instantiation of the data at each computing entity depends on the capabilities of the entity.

40. A method as claimed in claim 33, in which the rules define at least one item selected from:

a. the purpose for which the data can be used

b. the geographical area in which the data may be manifested

c. the temporal domain in which the data may be manifested

d. the computing platforms that may manipulate the data.

41. A method as claimed in claim 33 in which the data further includes test data, the test data is comparable to the structure of real data contained by the data items, and in which the results of operations performed on the test data are examined in order to make a decision on whether to release the real data to node that operated on the test data.

42. A method as claimed in claim 33, in which a computing entity finding itself in possession of data whose history or content do not meet predetermined requirements, or wishing to make data

available because it has performed some processing in at least partially masked form, formats the data places it in a repository.

43. A computer program stored on computer readable media for instructing a programmable computer to implement a method of controlling the processing of data, wherein the data comprises a plurality of usage rules for a plurality of data items, the programmable computer being programmed to apply individualised usage rules to each of the data items based on a measurement of integrity of a computing entity to which the data items are to be made available, the computer program permitting instantiation of the data items at the computing entity only if the integrity of the computing entity complies with the individualised usage rules associated with said data items.

Claims 44 - 49. Cancelled.

50. A computer apparatus for controlling processing of data, wherein the data comprises a plurality of usage rules for a plurality of data items stored by said computer apparatus, said computer apparatus controlling instantiation of the data at a computing entity, said computer apparatus including:

programming for applying individualised usage rules to each of the data items based on a measurement of integrity of the computing entity to which the data items are to be made available, said data items being logically grouped together as a set of data items, and

programming for individually instantiating data items in the set of data items at the computing entity as a function of

the integrity of the computing entity and the usage rule applicable to each data item in said set.

No evidence is being submitted

No copies of decisions rendered in related proceedings are being submitted.